Clarification of the cyclic code shift

We said that a for a cyclic code of length n the polynomial computations have to be carried out in arithmetics modulo $x^n \oplus 1$.[1] Recalling the definitions of modular arithmetics and congruence relations it is easy to demonstrate that

$$x^n \oplus 1 \equiv 0 \pmod{x^n \oplus 1} \iff x^n \equiv 1 \pmod{x^n \oplus 1}$$

and therefore also

$$\begin{aligned} x^{n+1} &\equiv x \pmod{x^n \oplus 1}, \\ x^{n+2} &\equiv x^2 \pmod{x^n \oplus 1}, \\ &\vdots \\ x^{n+n} &\equiv 1 \pmod{x^n \oplus 1}. \end{aligned} \tag{1}$$

Taking a generic binary polynomial

$$a(x) = a_{n-1}x^{n-1} \oplus a_{n-2}x^{n-2} \oplus \cdots \oplus a_1 x \oplus a_0$$

and multiplying it by x we get a shifted polynomial $a^{(1)}(x)$ as

$$x \cdot a(x) = a_{n-1}x^n \oplus a_{n-2}x^{n-1} \oplus \cdots \oplus a_1 x^2 \oplus a_0 x \equiv a^{(1)}(x)$$

and as all computations are carried out modulo $x^n \oplus 1$ we have

$$\begin{aligned} a^{(1)}(x) &\equiv a_{n-1} \cdot x^n \oplus a_{n-2}x^{n-1} \oplus \cdots \oplus a_1 x^2 \oplus a_0 x \pmod{x^n \oplus 1} \\ &\equiv a_{n-1} \cdot 1 \oplus a_{n-2}x^{n-1} \oplus \cdots \oplus a_1 x^2 \oplus a_0 x \pmod{x^n \oplus 1} \\ &\equiv a_{n-2}x^{n-1} \oplus \cdots \oplus a_1 x^2 \oplus a_0 x \oplus a_{n-1} \pmod{x^n \oplus 1}. \end{aligned}$$

In practice we can either directly replace the x^n by 1, x^{n+1} by x and so on as suggested by Equations (1), or we can add another $a_{n-1}(x^n \oplus 1) = a_{n-1}x^n \oplus a_{n-1}$ to the polynomial as the value of this expression is eqivalent (congruent) to zero in arithmetic modulo $x^n \oplus 1$.

Example 1. *Let us first study the shift of a codeword*

$$v = (1101010), \; v(x) = x^6 \oplus x^5 \oplus x^3 \oplus x.$$

of a binary cyclic code with $n = 7$.

The shifted codeword shall be $v^{(1)} = (1010101)$. *Multiplying* $v(x)$ *by* x *we get*

$$\begin{aligned} v^{(1)}(x) = x \cdot v(x) &= x^7 \oplus x^6 \oplus x^4 \oplus x^2 \pmod{x^7 \oplus 1} \\ &\equiv 1 \cdot (x^7 \oplus 1) \oplus 1 \cdot x^7 \oplus x^6 \oplus x^4 \oplus x^2 \pmod{x^7 \oplus 1} \\ &\equiv x^7 \oplus x^7 \oplus x^6 \oplus x^4 \oplus x^2 \oplus 1 \pmod{x^7 \oplus 1} \\ &\equiv x^6 \oplus x^4 \oplus x^2 \oplus 1 \pmod{x^7 \oplus 1}. \end{aligned}$$

The value of $v_6 = 1$ *and the added* $v_6(x^7 \oplus 1)$ *transforms the outlying* x^7 *into* 1. *We can see that the resulting codeword polynomial* $x^6 \oplus x^4 \oplus x^2 \oplus 1$ *indeed corresponds to* (1010101).

[1] In fact we are computing in modulo $x^n - 1$, but remember that in our arithmetics $+1 = -1$ and therefore $x^n - 1 = x^n + 1$.

Example 2. *Let us now have a look at a codeword that does not have the most-significant bit set, for example a codeword*

$$v(x) = (0101010) = x \oplus x^3 \oplus x^5$$

of a binary cyclic code again with $n = 7$.

The shifted codeword shall be $v^{(1)} = (0010101)$. *Multiplying* $v(x)$ *by* x *we get*

$$\begin{aligned} v^{(1)}(x) = x \cdot v(x) &= x^2 \oplus x^4 \oplus x^6 \\ &\equiv x^2 \oplus x^4 \oplus x^6 \oplus 0 \cdot (x^7 + 1) \ (mod\, x^7 \oplus 1) \\ &\equiv x^2 \oplus x^4 \oplus x^6 \oplus 0 \cdot 0 \ (mod\, x^7 \oplus 1) \\ &\equiv x^2 \oplus x^4 \oplus x^6 \ (mod\, x^7 \oplus 1). \end{aligned}$$

In this case $v_6 = 0$ *and the added* $v_6(x^7 \oplus 1)$ *does not influence the shifted polynomial. The resulting codeword polynomial* $x^2 \oplus x^4 \oplus x^6$ *indeed corresponds to* (0010101).